PAT-NO: JP410074182A

DOCUMENT-IDENTIFIER: JP 10074182 A

TITLE: ELECTRONIC SECRET VOTING METHOD

PUBN-DATE: March 17, 1998

INVENTOR-INFORMATION:
NAME
OKAMOTO, TATSUAKI

ASSIGNEE-INFORMATION:
NAME COUNTRY
NIPPON TELEGR & TELEPH CORP <NTT> N/A

APPL-NO: JP08230869

APPL-DATE: August 30, 1996

INT-CL (IPC): G06F015/00, G06F019/00 , G09C001/00

ABSTRACT:

PROBLEM TO BE SOLVED: To prevent the proof of voting from being prepared.

SOLUTION: A voter V<SB>i</SB> enciphers a voting content v<SB>i</SB> by using a random number r<SB>i</SB>, a blind signature s<SB>i</SB> by an election manager is applied to m<SB>i</SB>=E(v<SB>i</SB>, r<SB>i</SB>), and (m<SB>i</SB>, s<SB>i</SB>) is transmitted to a list display, voting is executed, and it is opened to public. In the enciphering method E, the voter V<SB>i</SB> can calculate (v<SB>i</SB>', r<SB>r</SB>')(v<SB>i</SB>≠v<SB>i</SB>') from which E(v<SB>i</SB>, r<SB>i</SB>)=E(v<SB>i</SB>', r<SB>i</SB>') can be obtained by using his own secret information a<SB>i</SB>. The voter V<SB>i</SB> transmits the voting content v<SB>i</SB>, the random number r<SB>i</SB>, and the above mentioned

m<SB>i</SB> to a collector C, and the collector C obtains
v<SB>i</SB>,...,
v<SB>b</SB> in a random sequence v<SB>i</SB>',..., v<SB>b</SB>', and
calculates
information σfor certifying that the v<SB>i</SB>(i=1,..., b) is
any
correct voting content of (m<SB>i</SB>,..., m<SB>b</SB>), and opens
it to
public.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－74182

(43)公開日　平成10年(1998) 3月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ｚ	
19/00		7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｚ	
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ		６６０Ｇ	
			Ｇ０６Ｆ　15/28	Ｂ	

審査請求　未請求　請求項の数２　ＯＬ　（全 5 頁）

(21)出願番号　特願平8－230869

(22)出願日　平成８年(1996) ８月30日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　岡本　龍明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　電子無記名投票方法

(57)【要約】

【課題】　投票の証拠が作れないようにする。

【解決手段】　投票者V_iは投票内容v_iを乱数r_iを用いて暗号化し、その$m_i = E(v_i, r_i)$に対し選挙管理者によるブラインド署名s_iを付け、(m_i, s_i)を一覧表示器へ送り投票して公開される。暗号化法EはV_iが自分だけの秘密情報a_iを用いて$E(v_i, r_i) = E(v_i', r_i')$となる$(v_i', r_i')$　$(v_i \neq v_i')$を計算できるものである。V_iはv_i, r_i, m_iを集計者Cへ送り、Cはv_i, …, v_bをランダムな順序v_i', …, v_b'とし、そのv_i　$(i = 1, \cdots, b)$は$(m_i, \cdots, m_b)$の何れかの正しい投票内容であることを証明する情報σを求めて公開する。

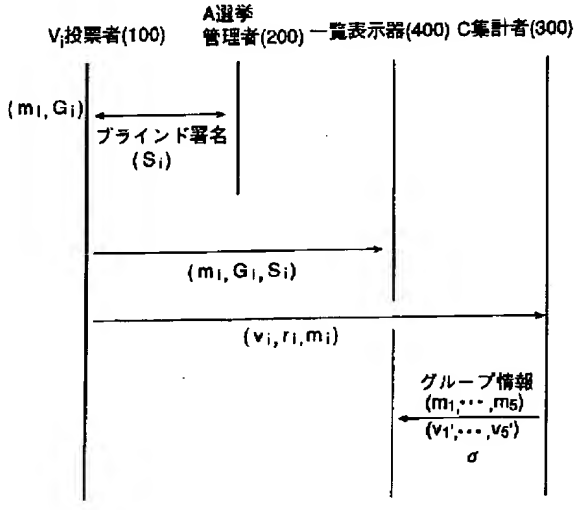

図　2

1

【特許請求の範囲】

【請求項1】　投票者V_i の投票者装置と、選挙管理者の選挙管理者装置と、集計者の集計者装置とにより電子的に無記名投票を実現する方法において、

投票者V_i 装置は、投票内容v_i を乱数r_i を用いて$m_i = E(v_i, r_i)$に暗号化し、

自分だけがもつ秘密情報a_i を用いることにより$E(v_i, r_i) = E(v_i'', r_i'')$となるような$(v_i'', r_i'')$ $(v_i \neq v_i'')$を計算し、m_iを投票することを特徴とする電子無記名投票方法。

【請求項2】　投票者V_i 装置は、m_i を表示器へ送り、

表示器は投票$(m_1, \cdots, m_b)$を公開し（bは投票者総数）投票者V_i 装置は集計者装置に秘密に(v_i, r_i)を送付し、

集計者装置は、$v_1, \cdots, v_b$ をランダムな順序$v_1', \cdots, v_b'$とし、さらにいずれのv_i' $(i = 1, \cdots, b)$も$(m_1, \cdots, m_b)$のいずれかの正しい投票内容であることを証明する情報σと$v_1', \cdots, v_b'$を上記表示器に公開することを特徴とする請求項1記載の電子無記名投票方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子的手段を用いて投票やアンケート調査等を行う場合に、安全で、かつ、公平な無記名投票を実現しようとする電子無記名投票方法に関する。

【0002】

【従来の技術】電子無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシーを守るのに適しているので、電子会議やＣＡＴＶ等の双方向通信での投票、アンケート調査等に利用できる。電気通信において、安全で、かつ、公平な無記名投票を行うには、投票者の偽装や二重投票、投票文の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、ディジタル署名を用いた電子投票方法が提案されており、例えば、太田和夫：“単一の選挙管理者を用いた電子投票方式”、昭和６３年電子情報通信学会春季全国大会、Ａ－２９４（昭６３－３）がある。

【0003】しかしながら、この方法には、次のような欠点が存在する。投票者の選挙内容が（無記名で）掲示板などに公開され、投票者本人には他の投票と簡単に識別できる。この特徴は自分の投票が無視されたとき（公開されないとき）、異議申し立てを行うことを可能とし、選挙結果の正当性を保証することに役立つ。

【0004】しかし、この特徴は反面、投票者本人しか知らない情報を投票の証拠として使えることを意味する。つまり、投票者を買収し、買収された投票者が言われた通りの投票を行ったことを証明するために、投票の

2

証拠が使われる危険がある。また、脅迫等により投票を強要することにも使われる危険がある。

【0005】

【発明が解決しようとする課題】この発明の目的は、投票の証拠が作れない安全な電子無記名投票方法を提供することにある。

【0006】

【課題を解決するための手段】この発明では、２つの技術を用いる。１つは、請求項１の発明に用いるもので秘密情報を持っていれば幾通りにも復号が可能な暗号方法を用いている。つまり、投票者V_i は、投票内容v_i を乱数r_i を用いて$m_i = E(v_i, r_i)$に暗号化し、それが投票情報として公開されるが、投票者本人V_i は、自分だけがもつ秘密情報a_i を用いることにより$E(v_i, r_i) = E(v_i'', r_i'')$となるような$(v_i'', r_i'')$ $(v_i \neq v_i'')$を計算することができる。この性質により、投票者は、実際は(v_i, r_i)を投票したとしても、投票を買収する者に対して、(v_i'', r_i'')を投票したと偽った証拠を提示できる。従って、このような暗号関数Ｅを用いて、投票の証拠性を無くしている。

【0007】請求項２の発明ではＥが上記のような性質を持っていても、集計者が(v_i, r_i)を公開すれば、それが投票の証拠となる。このようなことを防ぐため、$m_i = E(v_i, r_i)$とv_i の対応関係を秘密にしたまま、v_i を開示する証明方法を採用している。

【0008】

【発明の実施の形態】以下では、この発明の一実施例について説明する。図１はこの発明が適用されるシステム構成例を示す。Ｉ人の投票者V_i の投票者装置１００は、選挙管理者Ａの管理者装置２００、集計者この集計者装置３００、一覧表示器４００とそれぞれ、通信路５００を介して結合されているとする。また、投票者は全員、一覧表示器４００にアクセスが可能であるとする。図２にこの発明の通信シーケンス例を示し、以下、それぞれ、図３に投票者装置１００の機能構成例を、図４に集計者装置３００の機能構成例を、図５に一覧表示器４００の掲示例をそれぞれ示す。

【0009】以下では、特に投票者V_i （$i = 1, 2, \cdots, I$）が投票内容v_i を選挙管理者Ａの承認を得た後に、集計者装置３００に対して投票する場合について説明する。以下、投票の手順を示す。まず、システムで共通に使うパラメータとして以下の条件を満足する値ｐ，ｑ，ｇ，ｈが定められているとする。ｐ，ｑ：素数

$q \mid p-1$　　（ｑはｐ－１の約数）

q，$h \in Z_p^*$（乗法群）で位数がｑ、つまり$g^q \equiv h^q \equiv 1 \pmod p$，でかつ$g \neq h \neq 1$とし、また、$a$（$h = g^a \bmod p$）の値は誰も知らないものとする（例えば、一般に公開された疑似乱数生成アルゴリズムを使ってｇ，ｈを独立に生成する）。

3

【0010】1．投票者V_iの投票者装置100は、投票の準備を以下のように行う。まず乱数生成器101を使って、$a_i \in Z_q$を生成し、剰余演算器102を使って、$G_i = g^{a_i} \bmod p$を計算する。次に、投票者V_iは、投票内容v_iを定めて、投票者装置100に入力し、投票者装置100は乱数生成器101を用いて乱数r_iを生成し、剰余演算器103を使って、

$m_i = BC(v_i, r_i) = g^{v_i} G_i^{r_i} \bmod p$,

を計算する。

【0011】2．投票者V_i装置100は、ブラインド署名の手法(David Chaum:"Securitywithout identification: Transaction systems to make big brother obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044 (Oct.,1985) に記述されている) を用いて、(m_i, G_i)に対する選挙管理者装置200の署名s_iを得る。

【0012】3．投票者V_i装置100は(m_i, G_i, s_i)を一覧表示器400に匿名で送付し、掲示する。また、投票者V_i装置100は、集計者装置300に(v_i, r_i, m_i)を秘密に(例えば、暗号通信で)送る。

4．集計者装置300は、適当に投票者のグループ分けをして、各グループに全ての(ほとんどの)候補者が投票内容に含まれているようにする。例えば、以下では説明を簡単にするために5人の投票者からなるグループについて説明を行う。

【0013】この例では、一覧表示器400で掲示されているものとしては$((m_1, G_1), \cdots, (m_5, G_5))$がこのグループに対応することが集計者装置300により宣言される。さらにその投票内容$(v_1, v_2, v_3, v_4, v_5)$がランダムな順序で集計者装置300により公表される。ここで、順序をランダムにする置換をπとして、公表された投票内容を$v_1', v_2', v_3', v_4', v_5' = \{\pi(v_1), \pi(v_2), \cdots, \pi(v_5)\}$と表現する。例えば、置換$\pi$を$(1, 2, 3, 4, 5) \rightarrow (2, 4, 1, 5, 3)$とすると、$(v_1', v_2', v_3', v_4', v_5') = (v_2, v_4, v_1, v_5, v_3)$となる。なお、$\pi$は集計者装置300のみが知っている秘密である。

【0014】5．集計者装置300は以下の方法で$(v_1', v_2', v_3', v_4', v_5')$が正しい投票内容であることを$\pi$, $(r_1, \cdots, r_5)$を秘密にしたまま、その証明となる情報σを公表する。以下、σの生成方法を示す。集計者装置300は、5個の要素を並べ替える置換δ_jを、乱数生成器301を使ってランダムにk個$(j = 1, \cdots, k)$を選び、さらに乱数$u_{ij}, s_{ij}, t_{ij} \in Z_q$ $(i = 1, \cdots, 5; j = 1, \cdots, k)$を選ぶ。

【0015】次に、剰余演算器302を使って以下を計算する。

4

$Z_{ij} = m_i G_i^{s_{ij}} h^{u_{ij}} \bmod p$,

$W_{ij} = g^{v'_i} h^{t_{ij}} \bmod p$,　$i = \delta_j(i)$

$(i = 1, \cdots, 5 \; j = 1, \cdots, k)$

次に、Fを任意の長さのデータをkビットに圧縮する関数として、この関数演算器303を用いて、

$(e_1, e_2, \cdots, e_k) = F(Z_{11}, \cdots, Z_{5k}, W_{11}, \cdots, W_{5k})$

を求める。ここで、$e_j \in \{0, 1\}$ $(j = 1, \cdots, k)$。

【0016】次に、e_jの値に応じて比較器305を用いて判断を行い、$e_j = 0$ $(j = 1, \cdots, k)$ならば、$Y_j = (\delta_j, u_{ij}, s_{ij}, t_{ij}(i = 1, \cdots, 5))$とし、$e_j = 1$ $(j = 1, \cdots, k)$ならば、集計者装置300は、置換演算器304、剰余演算器306を用いて、

$\rho_j = \pi^{-1} \circ \delta_j^{-1}$,　(AoBは関数AとBの合成を示す)

$x_{ij} = r_i + s_{ij} \bmod p$,

$y_{ij} = u_{ij} - t_{\rho_j(i)} \bmod p$,

を計算し、$Y_j = (\rho_j, x_{ij}, y_{ij}(i = 1, \cdots, 5))$とする。

【0017】以上より、証明情報σを以下のように定める。

$\sigma = (Z_{11}, \cdots, Z_{5k}, W_{11}, \cdots, W_{5k}, Y_1, \cdots, Y_k)$

6．証明情報σの正当性の検証は以下のように行う。(以下では、投票者装置100が検証を行う例で説明する。)

まず、Fの関数演算器104にσの$(Z_{11}, \cdots, Z_{5k}, W_{11}, \cdots, W_{5k})$を入力して$(e_1, e_2, \cdots, e_k)$を求める。

【0018】次に、e_jの値に応じて比較器106を用いて判断を行い、$e_j = 0$ $(j = 1, \cdots, k)$ならば、剰余演算器107、比較器108を用いて

$Z_{ij} = m_i G_i^{s_{ij}} h^{u_{ij}} \bmod p$,

$W_{ij} = g^{v'_i} h^{t_{ij}} \bmod p$,　$i' = \delta_j(i)$

$(i = 1, \cdots, 5)$であることを確認する。

【0019】$e_j = 1$ $(j = 1, \cdots, k)$ならば、投票者装置100は、剰余演算器109、比較器110を用いて、

$W_{i'j} G_i^{x_{ij}} h^{y_{ij}} \equiv Z_{ij} \pmod p$,　$i' = \rho_j(i)$

が成立するかどうかを検証する。上述において、選挙管理者装置による署名は必ずしも必要としない。

【0020】

【発明の効果】まず、請求項1の発明では$m_i = BC(v_i, r_i) = g^{v_i} G_i^{r_i} \bmod p$では、投票者本人$V_i$は、自分だけがもつ秘密情報$a_i$ $(G_i = g^{a_i} \bmod p)$を用いることにより$m_i = g^{v_i} G_i^{r_i} \bmod p$を定めた後に、任意の$v_i' \in Z_q$に対して

5

$m_i = g^{v_i} G_i^{r_i} \bmod p = g^{v_i'} G_i^{r_i'} \bmod p$ となるような $r_i' \in Z_q$ を計算することができる。従って、投票者は、実際は（v_i，r_i）を投票したとしても、投票を買収する者に対して、任意の $v_i'' \in Z_q$ を投票したとする偽った証拠（v_i''，r_i''）を提示できる。

【００２１】さらに、集計者は投票の証拠となる r_i を秘密にして、m_i と v_i の対応関係も秘密にしたままであるため、投票の証拠性が無いことになる。一方、請求項2の発明では集計者はσを公開することにより、$m_i = BC(v_i, r_i)$ と v_i の対応関係を秘密にしたまま、v_i が正しい投票内容であることを証明しており、このような証明を付けたとき集計者は不正な投票内容 v_i^* を公開することはほぼ不可能である。つまり集計者の投票内容を変更するなどの不正を検証することができる。

6

【図面の簡単な説明】

【図１】この発明方法が適用されるシステム構成例を示すブロック図。

【図２】この発明方法のシーケンス例を示す図。

【図３】投票者装置１００の機能構成例を示すブロック図。

【図４】集計者装置３００の機能構成例を示すブロック図。

【図５】掲示例を指す図。

【図1】

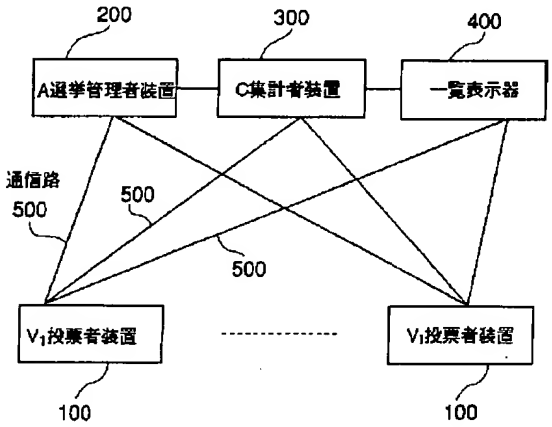

図　1

【図2】

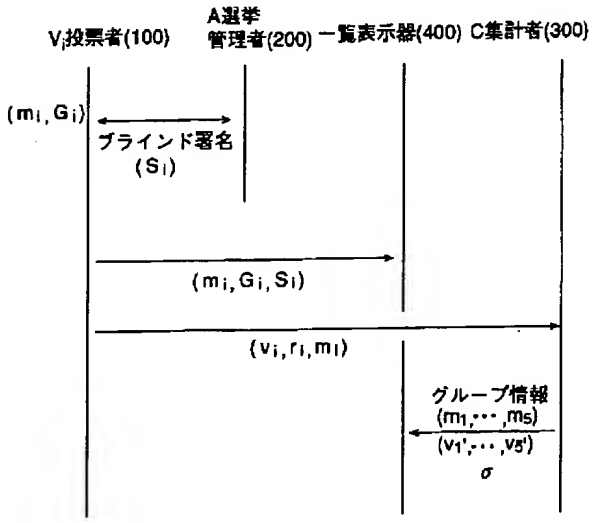

図　2

【図5】

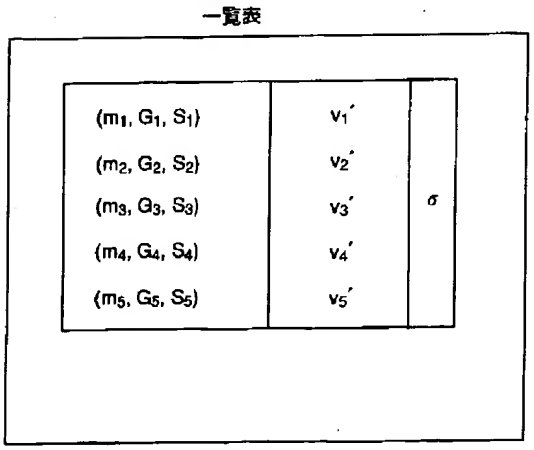

図　5

【図3】

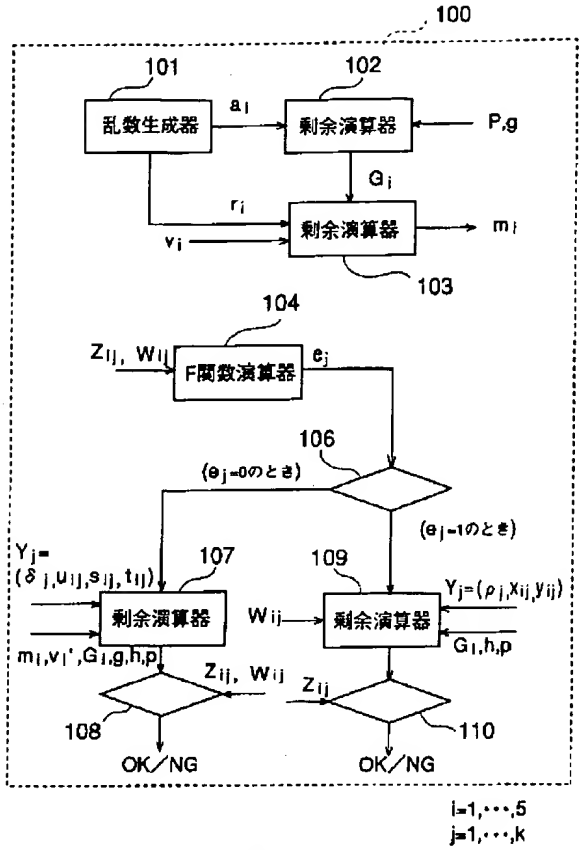
100
101
102
乱数生成器
剰余演算器
P,g
Gi
ri
剰余演算器
mi
vi
103
104
Zij, Wij
F関数演算器
ej
106
(ej=0のとき)
(ej=1のとき)
Yj=
(δj,uij,sij,tij)
107
109
剰余演算器
Wij
剰余演算器
Yj=(ρj,xij,yij)
Gi,h,p
mi,vi',Gi,g,h,p
Zij, Wij
Zij
108
110
OK／NG
OK／NG
i=1,･･･,5
j=1,･･･,k

図　3

【図4】

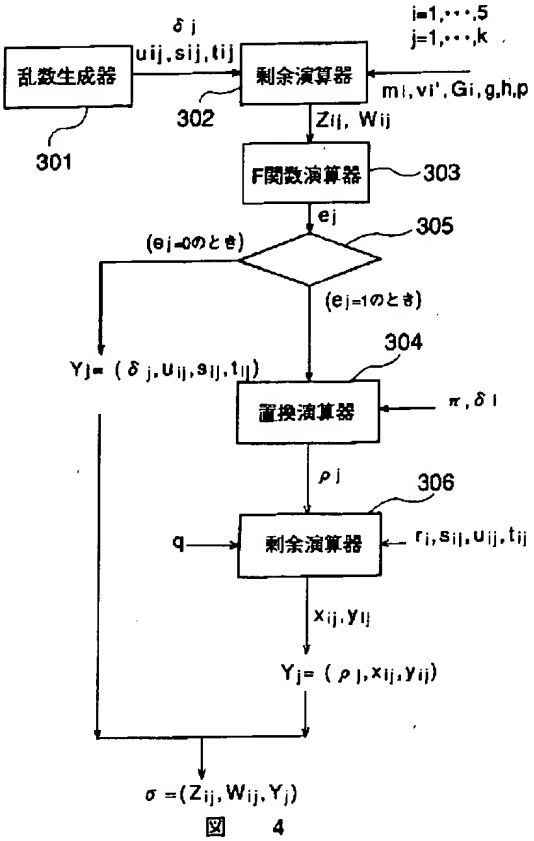
δj
i=1,･･･,5
j=1,･･･,k
乱数生成器
uij,sij,tij
剰余演算器
mi,vi',Gi,g,h,p
301
302
Zij, Wij
F関数演算器
303
ej
(ej=0のとき)
305
(ej=1のとき)
Yj=（δj,uij,sij,tij）
304
置換演算器
π,δi
ρj
306
q
剰余演算器
ri,sij,uij,tij
xij,yij
Yj=（ρj,xij,yij）
σ=(Zij,Wij,Yj)

図　4